UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/659,864	09/12/2000	J. Leslie Vogel III	0044860.P2436	5866

45217 7590 02/09/2009

APPLE INC./BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
02/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/659,864	VOGEL, J. LESLIE	
	Examiner	Art Unit	
	TONGOC TRAN	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *52-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *52-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on 11/24/2008. Claims 52 are pending for examination.

Response to Arguments

2. Applicant's arguments filed 11/24/2008 have been fully considered but they are not persuasive.

Applicant contends that Quick explicitly teaches away from including an encrypted password in the message in order to protect the password. Therefore, in view of such discouragement from Quick, one of ordinary skill in the art would not have been motivated to modify Lewis by Quick and Schneier.

Examiner submits that the concept of encrypting sensitive data when transmitting over un-secure network using any form of encryption algorithms is not new. Quick emphasizes that concept by stating that "[i]t is evident that the password must be protected from compromise during the registration process, otherwise the subscription information would be subject to cloning by fraudulent users who obtain the user identifier and password." (Quick, col. 2, lines 45-48). Quick illustrates the work of Bellovin and Merritt to provide the techniques for securely verify that the terminal and wireless network both know the correct password without revealing the password. By suggesting that both the terminal and the wireless network know the correct password, the password has to be securely exchanged at one point. The cited portion where Quick indicated that "[i]f the password is not included *in the message*, even in encrypted

form, then it is more difficult to be compromised. "The message" refers throughout Quick to be key information (i.e. Diffie-Hellman's SKE or EKE messages). The idea of not transmitting the password along with the key information as Quick suggested here, even when the password is encrypted, would make it more difficult to be compromised because if the password is compromised, it would compromised the key information (the message) sending along with the password. In addition, user name and password are commonly used as authentication information to verify the identity of the user and having this information transmitted over the network encrypted would have been well known. In the Specification, Applicant's user and password transmitted encrypted also serves the commonly known purpose of authenticating the identity of the mobile user (e.g. page 21, lines 1-3).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 52-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (U.S. Patent No. 6,526,506) in view of Quick, Jr. (U.S. Patent No. 6,178,506, hereinafter Quick) and further in view of Schneier ("Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc. 1996, hereinafter Schneier) .

With respect to claims 52, 54-56, 59-66 and 68-70, Lewis discloses a computerized method, a computer-readable medium and a wireless network of establishing a secure wireless communication channel between an access point and a station, the channel being encrypted with a channel key, comprising:

the access point receiving a connection request from the station to initiate a setup connection between the access point and the station (e.g. Lewis, col. 10, lines 47-61, conventional initialization routine, mobile terminal seek out access point);

the access point sending a shared key to the station in response to the connection request if the access point is capable of handling a connection to the station (e.g. Lewis, col. 10, lines 59-61 and col. 12, lines 35-47, encryption in basic registration, encrypt key);

Lewis does not disclose the user name and password is encrypted with self-distributed key. However, Quick discloses when communicating with access point, mobile terminal user should protect secrecy of password, either in encrypted form or not (e.g. col. 4, lines 36-37). Schneier discloses the Hughes encryption scheme for generating self-distributed key (Schneier, page 515, Alice - Access point, Bob - Station, self-distributed key - K=K'). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the Hughes encryption scheme to protect the password by taking the advantage of exchanging keying information without the key to protect the password from being compromised.

With respect to claims 53, 57, 58, 67, 71 and 72, further comprising:

The access point encrypting the channel key using the self-distributed key if the user name and the password are valid; and

The access point sending the encrypted channel key to the station to cause the station to terminate the setup connection and to establish a secure connection with the access point using the channel key (e.g. Lewis, col. 9, lines 24-40).

Conclusion

4, **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TONGOC TRAN whose telephone number is (571)272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tongoc Tran/
Examiner, Art Unit 2434